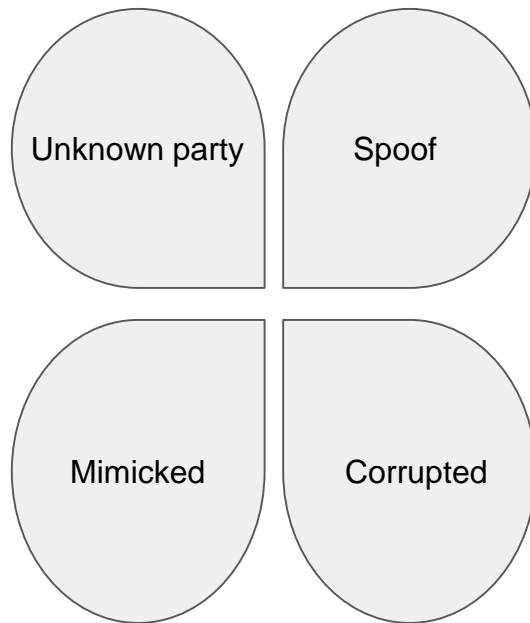
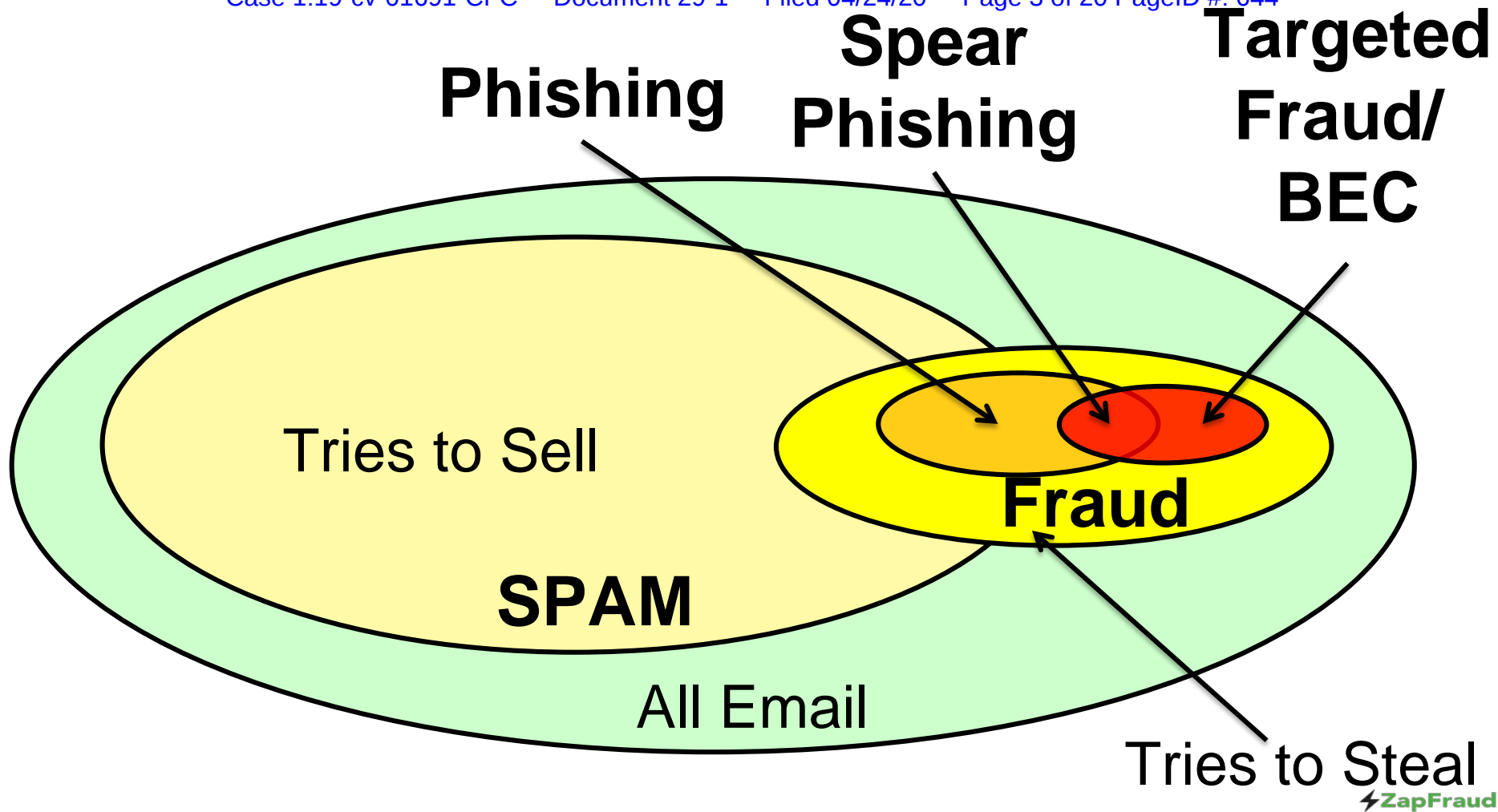


# **EXHIBIT A**

# ZapFraud Fraud Detection



Proofpoint, December 2 2015



# Traditional filtering treats the symptoms, not the disease.



Treating *spam* symptoms does little good when the disease is *BEC*.

# Fraud Firewall™

Stops fraud at the perimeter

Extensible framework with many proprietary filters

Learns from fraudulent communication

Configured by tunable rules

Customizable to segment needs

Based on analysis of meaning

# What does ZapFraud do?

## 1. Identify the *meaning* of things

a. Do two parties *trust* each other?

(Having responded does not mean they do!)

b. Are there *deceptive* headers or content?

(Meaning and apparent meaning do not align.)

c. Does the content match a known high-risk *storyline*?

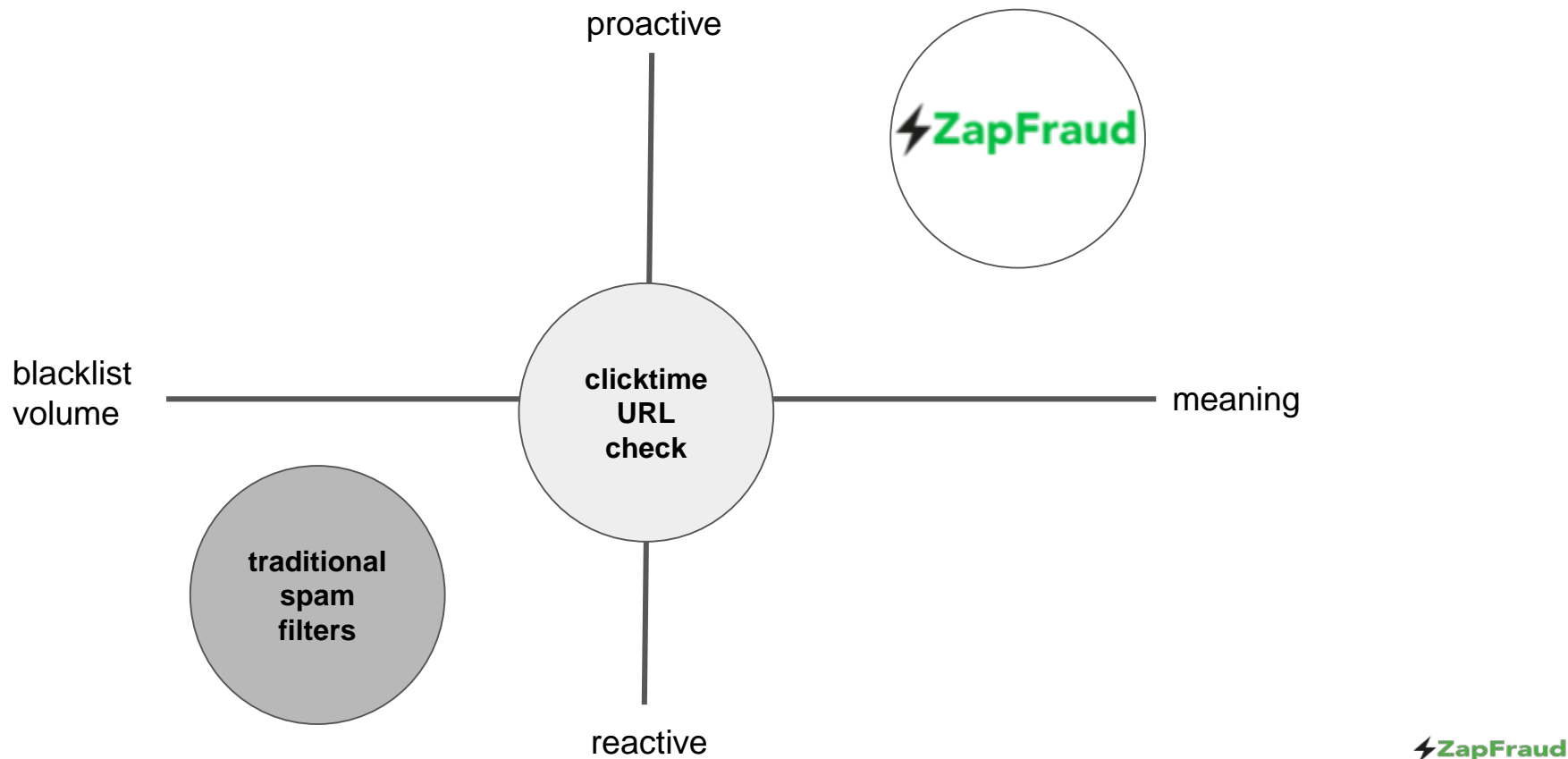
## 2. *Manage* based on the meaning - that minimizes error rates

a. Address common masquerade attacks










b. Address common account-takeover attacks

c. Address based on known fraudulent storylines

# ZapFraud addresses low-volume targeted scam.



# What do we address?

Attack	Traditional methods		ZapFraud Approach
Business from unknown party			Storyline?
Sender spoofing known party			Deceptive address? Storyline? Reply-to? Auth issues? Block/alert!
Sender mimicking known party			Trusted sender? Deceptive address? Storyline? Block!
Sender corrupting known party			Deceptive reply-to address? Storyline? Alert!

Traditional  
filters do not  
flag this.

# Examples of what we catch.

Not a  
blacklisted  
sender.

**From:** Wells Fargo Online <alerts@notify-wellsfargo.com>  
**Subject:** Wells Fargo online statement ready to view  
**Date:** July 3, 2015 at 2:06:07 PM GMT+7  
**To:** [markus.jakobsson@gmail.com](mailto:markus.jakobsson@gmail.com)



[wellsfargo.com](http://wellsfargo.com)

## Your new statement is now available online

The new statement for your Wells Fargo deposit account XXXXXX2619 is now available to view online.

URL is not  
blacklisted.

To view your statement from a browser:

- 1 Go to [Statements and Documents](#).
- 2 Select **Statements and Disclosures**.

3 Choose your account from the dropdown menu.

To view your statement from the Wells Fargo tablet app:

- 1 Sign on from the app.
- 2 Find this account in your Account Summary.
- 3 Select the View Statements link for this account.

If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements online, Wells Fargo Customer Service is available 24 hours a day, 7 days a week. Call us at 1-800-956-4442 or sign on to send a secure email.

Contains no  
blacklisted  
content.

# Examples of what we catch.

From: Wells Fargo Online <alerts@notify-wellsfargo.com>  
Subject: Wells Fargo online statement ready to view  
Date: July 3, 2015 at 2:06:07 PM GMT+7  
To: markus.jakobsson@gmail.com

Not trusted by recipient, and cousin-name with sender who is trusted.

Display name is deceptive since matches trusted sender, which is not actual sender.

 [wellsfargo.com](http://wellsfargo.com)

**Your new statement is now available online**

The new statement for your Wells Fargo deposit account XXXXXX2619 is now available to view online.

A “storyline” matching a whitelisted brand - which is not the apparent sender.

URL is not blacklisted, but does not match domain of brand matching storyline or display name.

To view your statement from a browser:

- 1 Go to Statements and Documents.
- 2 Select **Statements and Disclosures**.

3 Choose your account from the dropdown menu.

To view your statement from the Wells Fargo tablet app:

- 1 Sign on from the app.
- 2 Find this account in your Account Summary.
- 3 Select the View Statements link for this account.

If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements online, Wells Fargo Customer Service is available 24 hours a day, 7 days a week. Call us at 1-800-956-4442 or sign on to send a secure email.

Traditional  
filters do not  
flag this.

# Examples of what we catch.

**From:** Roger Harris <[Roger-Harris@hotmail.com](mailto:Roger-Harris@hotmail.com)>  
**Subject:** Lost my SecuriD token, need help quickly  
**Date:** July 9, 2015 at 1:16:27 PM GMT+7  
**To:** [linda.everts@lawyersrus.com](mailto:linda.everts@lawyersrus.com)

---

Not a  
blacklisted  
sender.

Linda,

I arrived now, and am getting ready for the meeting, but I have misplaced both my phone and my SecuriD token. I need your help, or this will be a fiasco! Please send me all the files you have about the meeting, especially the year-end numbers. I really need those. If you do not have the most recent versions of the docs, the old ones are better than nothing.

Since I cannot log in to my work account without the token, please send it to my personal account. Would you also check if I forgot the token on my desk and let me know? If it is not there, I will call and disable it, just in case I dropped it somewhere.

Please send the stuff right away, I am a bit panicked.  
I'll let you know how things go.

Roger

Contains no  
blacklisted  
content.

# Examples of what we catch.

Display name is deceptive since matches trusted sender, which is not actual sender.

From: Roger Harris <Roger-Harris@hotmail.com>  
Subject: **Lost my SecurID token, need help quickly**  
Date: July 9, 2015 at 1:16:27 PM GMT+7  
To: [linda.everts@lawyersrus.com](mailto:linda.everts@lawyersrus.com)

Not trusted by recipient, and user name is close match with sender who is trusted.

Linda,

I arrived now, and am getting ready for the meeting, but I have misplaced both my phone and my SecurID token. I need your help, or this will be a fiasco! Please **send me** all the files you have about the meeting, especially the year-end numbers. I really need those. If you do not have the most recent versions of the docs, the old ones are better than nothing.

Since I cannot log in to my work account without the token, please send it to my personal account. **Would you also check if I forgot the token on my desk and let me know?** If it is not there, I will call and disable it, just in case I dropped it somewhere.

Subject contains high-risk word.

Please send the stuff right away, I am a bit panicked.  
I'll let you know how things go.

Roger

Content portion contains high-risk words.

Traditional filters do not flag this.

# Examples of what we catch.

Not a blacklisted sender.

**From:** Liz, Gonzales <[EGonzalez@media-produtcion.com](mailto:EGonzalez@media-produtcion.com)>  
**Subject:** October invoice  
**Date:** October 29, 2015 at 9:10:17 AM GMT+8  
**To:** [Rudy.McCoy@glitz.com](mailto:Rudy.McCoy@glitz.com)

---

Dear Rudy,

Please find attached our invoice for the month of October. Please note the new banking details – we are staying with US Bank, but the bank updated our account number.

As always, we appreciate your business.

Regards,  
Liz

Contains no blacklisted content.

No malware detected in attachment.



invoice 44281

# Examples of what we catch.

From: Liz, Gonzales <EGonzalez@media-productcion.com>  
Subject: October invoice  
Date: October 29, 2015 at 9:10:17 AM GMT+8  
To: Rudy.McCoy@glitz.com

Not trusted by recipient, and cousin-name with sender who is trusted.

Display name is deceptive since matches trusted sender, which is not actual sender.

Dear Rudy,

Please find attached our invoice for the month of October. Please note the new banking details – we are staying with US Bank, but the bank updated our account number.

As always, we appreciate your business.

Regards,  
Liz

Subject contains high-risk word.



invoice 44281

Has an attachment, with a name containing high-risk word.

Attachment generated using free PDFconvert.

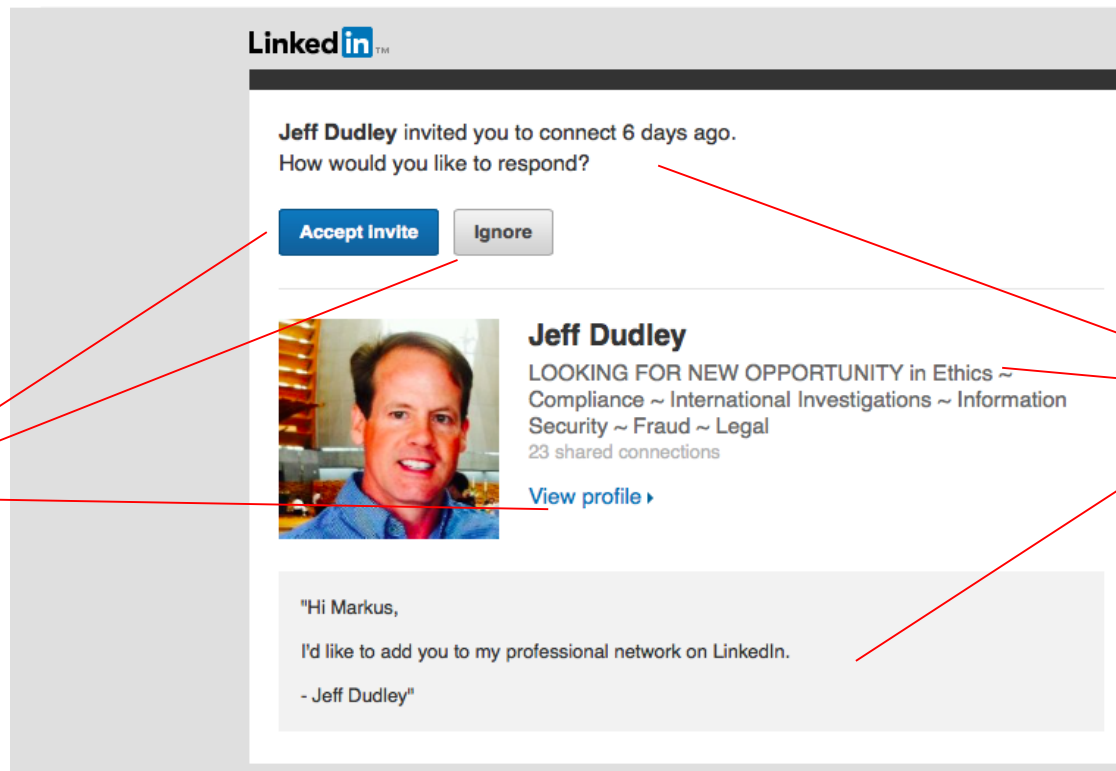
Content portion contains high-risk words.

Traditional  
filters do not  
flag this.

# Examples of what we catch.

Jeff Dudley <messages@noreply-linkedin.com>  
To: markus.jakobsson <markus.jakobsson@gmail.com>  
Jeff Dudley's invitation is waiting for your response

Not a  
blacklisted  
sender.



URL is not  
blacklisted.

Contains no  
blacklisted  
content.

# Examples of what we catch.

Jeff Dudley <messages@noreply-linkedin.com>  
To: markus.jakobsson <markus.jakobsson@gmail.com>  
Jeff Dudley's invitation is waiting for your response

Email address  
is deceptive  
since it is  
similar to  
trusted sender.

URLs do not  
match  
domain of  
brand matching  
storyline.

Not trusted by  
recipient.

A "storyline"  
matching  
a whitelisted  
brand - which is  
not the  
apparent  
sender.

LinkedIn

Jeff Dudley invited you to connect 6 days ago.  
How would you like to respond?

Accept Invite

Ignore



**Jeff Dudley**

LOOKING FOR NEW OPPORTUNITY in Ethics ~  
Compliance ~ International Investigations ~ Information  
Security ~ Fraud ~ Legal  
23 shared connections

[View profile](#)

"Hi Markus,

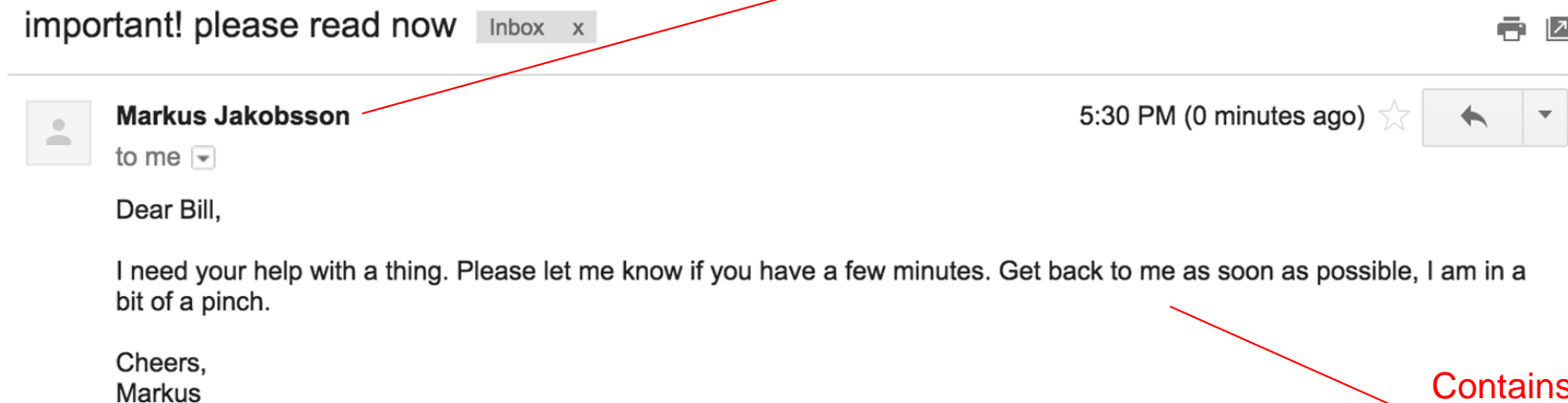
I'd like to add you to my professional network on LinkedIn.

- Jeff Dudley"

# Examples of what we catch.

Traditional filters do not flag this.

A common contact, and not a blacklisted sender.



Contains no blacklisted content.

# Examples of what we catch

(commonly not displayed) to a deceptive address, looking a lot like trusted party.

Trusted by recipient.

important! please read now

Inbox x



**Markus Jakobsson**

5:30 PM (0 minutes ago) ☆



to me ▾

Dear Bill,

I need your help with a thing. Please let me know if you have a few minutes. Get back to me as soon as possible, I am in a bit of a pinch.

Cheers,  
Markus

A storyline matching a common threat.

# Fraud Firewall™ - collaboration points

Stops fraud at the perimeter

**Extensible framework** with many proprietary filters

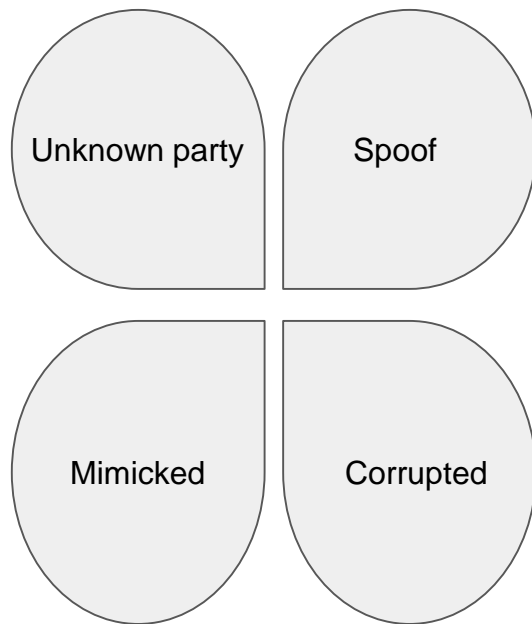
**Learns from fraudulent communication**

**Configured by tunable rules**

**Customizable to segment needs**

Based on analysis of meaning

# ZapFraud Fraud Detection



Proofpoint, December 2 2015